UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,822	03/06/2002	A. Kent Sievers	1565.006US1	7995

21186   7590   10/24/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/092,822	SIEVERS ET AL.
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _14 August 2006_.

2a) ☒ This action is **FINAL.**   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-20_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-20_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _06 March 2002_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a) ☐ All   b) ☐ Some * c) ☐ None of:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____.

        3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
     Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Applicant's arguments filed August 14, 2006, have been fully considered but they are not persuasive.

2.   Claims 1-20 are pending and have been examined. Claims 21-26 have been cancelled.

Response to Amendment

3.   The objections to claims 16 and 17 are withdrawn.

4.   The rejection of claims 21-26 under 35 U.S.C. 101 is withdrawn due to the cancellation of said claims.

5.   Applicant's arguments with respect to the prior art have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

6.   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7.   **Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hruska et al. (US Patent 6,195,587, hereinafter Hruska), and further in view of Ranger et al. (US Patent 6,393,568, hereinafter Ranger).**

Regarding claim 1, Hruska teaches a method to remotely validate an email message **(col. 3, lines 40-67)**, comprising:

- receiving, at a recipient, the email message in a first encrypted format from a sender of the email message, wherein the recipient is whom the email message is directed to for consumption **(col. 4, lines 1-45)**;

- transferring, from the recipient, the decrypted email message contents to a remote server **(col. 5, lines 1-60)**; and

- receiving, at the recipient, from the remote server a status flag, wherein a value associated with the status flag indicates whether the contents are free from a virus or are free from objectionable material as validated by the remote server **(col. 5, lines 40-60)**.

Hruska does not expressly disclose decrypting, at the recipient, contents of the email message from the first encrypted format, but does teach using encryption at the recipient **(col. 5, lines 40-60)**. However, Ranger does teach decrypting from first format /re-encrypting **(col. 3, lines 15-45)**. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have the first workstation of Hruska receive encrypted content and decrypt it, prior to sending it to the remote validation server. One of ordinary skill in the art would have been motivated to perform such a modification to provide encryption (confidentiality) to the transmission (Ranger, col. 1, lines 5-63).

Regarding claim 7, Hruska teaches a method to validate a data message **(col. 3, lines 40-67)**, comprising:

- receiving the data message from a client, wherein the data message was previously received at the client and sent from a sender of the data message to the client, and wherein the client is external and remote to the method and communicates with the method over a network by sending the data message for scanning, and wherein the client is who

the data message is directed to for consumption **(col. 4, lines 1-45, col. 5, lines 1-60)**;

- scanning the data message for viruses **(col. 5, lines 1-60)**; and

- sending a validation flag to the client, wherein the validation flag includes a value indicating whether the data message includes zero or more of the viruses **(col. 5, lines 40-60)**.

Hruska does not expressly disclose decrypting, at the recipient, contents of the email message from the first encrypted format, but does teach using encryption at the recipient **(col. 5, lines 40-60)**. However, Ranger does teach decrypting from first format /re-encrypting **(col. 3, lines 15-45)**. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have the first workstation of Hruska receive encrypted content and decrypt it, prior to sending it to the remote validation server. One of ordinary skill in the art would have been motivated to perform such a modification to provide encryption (confidentiality) to the transmission (Ranger, col. 1, lines 5-63).

Regarding claim 14, Hruska teaches an email system to validate an email message **(col. 3, lines 40-67)**, comprising:

- a local email set of executable instructions residing on a client; a remote validation set of executable instructions residing on a server **(col. 4, lines 1-45, col. 5, lines 1-60)**; and

- wherein the email message is received by the local email set of executable instructions from a sender, who intends the email message

for the client and the client is who the email message is directed to for

consumption, and then streams the email message to the remote

validation set of executable instructions located on the server in an

unencrypted format or in a different encrypted format from what was

received on the client from the sender and wherein the email message is

scanned **(col. 5, lines 1-60)** and

- a validation flag associated with a result of the scan is sent to the local

email set of executable instructions back on the client **(col. 5, lines 40-**

60).

Hruska does not expressly disclose decrypting, at the recipient, contents of the

email message from the first encrypted format, but does teach using encryption at the

recipient **(col. 5, lines 40-60)**. However, Ranger does teach decrypting from first format

/re-encrypting **(col. 3, lines 15-45)**. Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to have the first

workstation of Hruska receive encrypted content and decrypt it, prior to sending it to the

remote validation server. One of ordinary skill in the art would have been motivated to

perform such a modification to provide encryption (confidentiality) to the transmission

(Ranger, col. 1, lines 5-63).

Regarding claim 2, the combination of Hruska and Ranger teaches encrypting

the email message in a second encrypted format before transferring the email message

to the remote server (Ranger, column 3, lines 1-67, column 4, lines 1-67).

Regarding claims 3 and 15, the combination of Hruska and Ranger teaches

accessing the email message for use, if the value of the status flag indicates the remote

server validated the email message (Hruska, col. 5, lines 1-60).

Regarding claims 4 and 20, the combination of Hruska and Ranger teaches

using encryption and email messages (Ranger, abstract, col. 2, lines 25-67, col. 3, lines

1-67), but does not expressly disclose using the Secure Multipurpose Internet Mail

Extension (S/MIME) format. Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to use any other kind of

encryption that could be applied to the system of Hruska and Ranger. One of ordinary

skill in the art would have been motivated to perform such a modification to protect

content (Ranger, col. 1, lines 5-67, col. 7, lines 1-60, Hruska, col. 2, lines 1-48).

Regarding claim 5, the combination of Hruska and Ranger teaches wherein in

receiving the status flag, if the value of the status flag indicates the remote server

validated the email message, then subsequent accesses made to the email message

do not result in the email message being transferred to the remote server for validation

(Ranger, col. 3, lines 1-67, col. 6, lines 1-67, Hruska, col. 2 lines 25-55).

Regarding claim 6, the combination of Hruska and Ranger teaches wherein in

transferring the email message, the email message is streamed to the remote server

(Ranger, col. 5, lines 1-67, col. 6, lines 1-67, Hruska, col. 5, lines 40-67, col. 6, lines 1-

11).

Regarding claim 8, the combination of Hruska and Ranger teaches decrypting the data message before scanning the data message (Ranger, col. 3, lines 1-67, col. 4, lines 1-67).

Regarding claim 9, the combination of Hruska and Ranger teaches wherein in decrypting the data message, the data message is decrypted using a public key of the client (Ranger, col. 3, lines 1-67, col. 4, lines 1-67).

Regarding claim 10, the combination of Hruska and Ranger teaches wherein in receiving the data message, the data message is an email message and the client is an email client (Ranger, abstract, col. 2, lines 25-67).

Regarding claim 11, the combination of Hruska and Ranger teaches wherein in receiving the data message, the data message is received from an operating system residing on the client (Ranger, abstract, col. 2, lines 25-67, Hruska, col. 5, lines 40-67).

Regarding claim 12, the combination of Hruska and Ranger teaches wherein in scanning the data message, a scanning set of executable instructions is selectively executed to scan the data message for zero or more of the viruses (Ranger, abstract, col. 2, lines 25-67, col. 3, lines 1-67, Hruska, col. 4, lines 23-55).

Regarding claim 13, the combination of Hruska and Ranger teaches wherein in receiving the data message, the data message is received as a data stream from the client and scanned as the data stream is received (Ranger, col. 5, lines 1-67, col. 6, lines 1-67).

Regarding claim 16, the combination of Hruska and Ranger teaches wherein the scan validates the email message if the email messages are free of viruses (Ranger, col. 3, lines 1-67, col. 6, lines 1-67).

Regarding claim 17, the combination of Hruska and Ranger teaches wherein the local email set of executable instructions removes the data message if the flag indicates the scan did not validate the email message (Ranger, col. 3, lines 1-67, col. 6, lines 1-67, Hruska, col. 1, lines 50-67, col. 2, lines 1-15).

Regarding claim 18, the combination of Hruska and Ranger teaches wherein communications between the local email set of executable instructions and the remote validation set of executable instructions are secure (Ranger, col. 1, lines 1-67, col. 3, lines 1-67, Hruska, col. 5, lines 40-60).

Regarding claim 19, the combination of Hruska and Ranger teaches wherein public and private key pairs associated with the client and the server are used to encrypt and authenticate the communications (Ranger, col. 3, lines 1-67, col. 4, lines 1-67).

Conclusion

8.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.
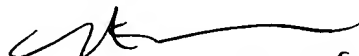
10.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

11.   Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/19/06